REMARKS

Claims 1-19, 24-30, and 32-50 are now pending in the application. Claims 20-23 and 31 have been canceled without prejudice or disclaimer. Claims 1, 4-5, 7-9, 19, 24, 28, 36, 44, and 48 have been amended without introduction of new matter. Favorable reconsideration is respectfully requested in view of the above amendments and the following remarks.

The Office's withdrawal of the restriction requirement is noted with appreciation.

Claim 48 was objected to because of the nonsensical phrasing "requested function cryptographic function". In response, claim 48 has been amended to remove the first occurrence of the word "function". As this amendment is believed to address the Office's concerned, withdrawal of the objection is respectfully requested.

Claims 7, 10-12, 14, 18, and 19 were rejected under 35 U.S.C. §101 for allegedly defining non-statutory subject matter. The Office objects that the subject claims define intangible subject matter in that they are directed to a device of which the claim language "comprising a cryptographic module" allows the device to be implemented solely in software (Specification, page 5). This rejection is respectfully traversed.

The fundamental test for patent eligibility is whether the claimed invention produces a "useful, concrete and tangible result." This test focuses on the result being tangible, not the claimed subject matter.

In determining whether claimed subject matter is statutory it should further be kept in mind that even if some aspects of the claims are considered to define intangible software signals, it is also well established that when an intangible signal is coupled with or combined with a statutory physical structure to produce a useful, concrete and tangible result, the combination constitutes statutory subject matter. Thus, for example, a claimed computer-readable medium encoded with a data structure defines structural and functional interrelationships between the data structure and the computer software and hardware components which permits the data structure's functionality to be realized, and is statutory. See, e.g., The U.S. Patent and Trademark Office's "35 U.S.C. 101 Training Materials" presented by Vincent Millin, Tariq Hafiz, Jim Trammell and Robert Olszewski (2005).

Independent claims 7 and 19 are believed to satisfy these requirements. As amended, claim 7 defines a mobile communications device comprising the cryptographic module in combination with "means for communicating" and "means for connection". Claims 10-12, 14, and 18 depend from claim 7, and therefore inherit these features as well. Independent

claim 19 has been amended to define, *inter alia*, "A tangible module for a personal computer...." These claims clearly set forth physical structures, and are therefore believed to define statutory subject matter at least because they satisfy the test of defining embodiments that achieve useful, tangible and concrete results, as required under Section 101. It is therefore respectfully requested that the rejection of claims 7, 10-12, 14, 18, and 19 under 35 U.S.C. §101 be withdrawn.

Claims 1, 4, 6, 19, 20, 24, 26-28, 31-34, 47, and 48 stand rejected under 35 U.S.C. §102(b) as allegedly being anticipated by Caputo et al. (U.S. Patent No. 5,778,071). This rejection is respectfully traversed.

Claims 20 and 31 have been canceled without prejudice or disclaimer, thereby rendering moot the rejection of these claims.

The remaining claims referenced in this rejection have been amended to even more clearly define relevant aspects of the invention. For example, independent claim 1 now defines "A method of encrypting communications from a computer having an application program interface, the method comprising initiating communications from said computer over a computer network; determining that encryption of said communications is required; establishing a connection with a mobile communications device, wherein said mobile communications device includes a cryptographic module for use in mobile communication over a wireless communications network; and using the cryptographic module of the mobile communications device as a cryptographic service provider for encrypting said communications from said computer over said computer network without sending said encrypted communications over said wireless communications network." (Emphasis added.) Support for this amendment may be found in the specification at, for example, Figs.1-3 and the supporting text spanning page 3 line, 19 through page 8, line 28.

Independent claim 19 has been similarly amended so that it now defines, *inter alia*, "the mobile communication device having a cryptographic module for use in mobile communication over a wireless communications network, such that the cryptographic module acts as a cryptographic service provider for said personal computer allowing the personal computer to communicate encrypted data over said computer network without sending data over said wireless communications network." (Emphasis added.)

Independent claim 28 has also been similarly amended so that it now defines "A method of encrypting communications from a computer having an application program

interface, wherein the communications are over a computer network", the method including, *inter alia*, "receiving encrypted data at the computer from the mobile communications device; and using the encrypted data in communications over the computer network without sending the encrypted data over the wireless communications network." (Emphasis added.)

Independent claim 24 has been amended to even more clearly define that the cryptographic module in the mobile communications device is "for performing cryptographic functions in mobile communication over a wireless communications network", and that the computer has at least one application which requires cryptographic functionality "for communication over a computer network." Claim 24 continues to define "the computer further comprising an interface device which, on determining that an application needs to use cryptographic functionality, selects the functionality provided in the computer, or the functionality provided in the mobile communications device, and sends a command thereto." (Emphasis added.)

Similarly, independent claim 47 continues to define a module for computer system "wherein, when the module receives from the application interface a request for a cryptographic function which the module is unable to provide, the module sends a command over the external interface to the mobile communications device to request the cryptographic function therefrom."

Embodiments defined by independent claims 1, 19, 24, 28, and 47 are believed to be patentably distinguishable over the prior art of record because they include novel and nonobvious features that enable a single mobile communications device to achieve a unique efficiency in that a same cryptographic module located in the mobile communications device is used not only to support the device's own communications with a wireless network, but also the cryptography requirements of a local external device, such as a personal computer having its own connection with a network as illustrated in FIG. 1. In this respect, it is important to understand that the personal computer is not communicating *through* the mobile communications device and the wireless network to get to its own network; its exchanges with the mobile communications device are for the purpose of utilizing the cryptographic functions that the mobile communications device can offer.

The Caputo et al. patent fails to disclose the combination of features defined by any of independent claims 1, 19, 24, 28, and 47 for a number of reasons. To begin with, the device disclosed by Caputo et al. is not "for use in mobile communication over a wireless

communications network" as variously required by the claims. Instead, the Caputo et al. device requires a wired connection to a network. (See, e.g., Fig. 2 and column 5, lines 62-65: "Further, the connector port 14 is a modular receptacle which may be directly connected to a data transfer path, such as a telephone system.") Furthermore, even if the Caputo et al. device were modified to be a mobile communications device communicating with a wireless network, the external device of Caputo et al. would not be capable of "initiating communications from said computer over a computer network ... without sending said encrypted communications over said wireless communications network"; instead, Caputo et al.'s computer is connected to the network *through* the device 10 (see, e.g., Caputo et al.'s figure 2). Moreover, the device of Caputo et al. appears to operate in only one mode, namely, for the benefit of the external device (computer); it sits in-between the computer and the network, passing data from one to the other, and performs cryptographic functions as required by the node that the *computer* is connected to. Consequently, there is no dual mechanism in which the cryptographic module of the mobile communication device is "for use in mobile communication over a wireless communications network" and also for "[acting] as a cryptographic service provider for said personal computer allowing the personal computer to communicate encrypted data over said computer network without sending data over said wireless communications network."

Caputo et al. also fails to disclose or suggest a division of cryptographic functions wherein some are performed within the computer itself and others are performed within a cryptographic module located in a mobile communications device so that the computer comprises "an interface device which, on determining that an application needs to use cryptographic functionality, selects the functionality provided in the computer, or the functionality provided in the mobile communications device, and sends a command thereto."

For the most part, the Office's remarks do not address the various features discussed above. The Office does allege, however, that the Caputo et al. patent, at column 15 lines 13-39, discloses a computer comprising an interface device which, on determining that an application needs to use cryptographic functionality, selects the functionality provided in the computer, or the functionality provided in the mobile communications device, and sends a command thereto. Applicant respectfully disagrees. The cited portion of Caputo et al. merely describes two modes of operation: one in which the device 10 encrypts the data and immediately sent it to the network 20, and another in which the device 10 performs the

encryption but then returns the encrypted data to the computer 22 for subsequent transmission to the network 20, possibly as part of another message. Nowhere does this passage describe a computer having its own cryptographic capabilities separate and apart from those provided by the device 10.

For at least the foregoing reasons, independent claims 1, 19, 24, 28, and 47 as well as the related dependent claims 4, 6, 26-27, 32-34, and 48, are believed to be patentably distinguishable over Caputo et al. Accordingly, it is respectfully requested that the rejection of these claims under 35 U.S.C. §102(b) be withdrawn.

Claims 2, 3, 7, 10-18, 21, 22, 25, 29, 30, 35-40, 42, and 44 stand rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over Caputo et al. in view of Grimm et al. (U.S. Patent No. 5,907,815) and further in view of Geiger et al. (U.S. Patent No. 6,463,534). This rejection is respectfully traversed.

Claims 21 and 22 have been canceled without prejudice or disclaimer, thereby rendering the rejection of these claims moot.

Of the remaining claims subject to this ground of rejection, claims 2, 3, 25, 29, 30, and 35 variously depend from one of the independent claims 1, 24, and 28 discussed above, and are therefore patentably distinguishable over Caputo et al. for the reasons set forth above. Independent claims 7, 36, and 44 similarly define features such as a mobile communications device including "a cryptographic module, the cryptographic module being usable: for encoding wireless communications from the device over said wireless interface; by a cryptographic service provider with an application program interface of the remote computer" (claim 7 and comparably defined in claim 44); and a system including a cryptography service provider in a computer, "wherein the cryptography service provider can obtain the cryptographic functionality, required by the application, from the cryptographic module of the mobile communications device without the mobile communications device sending the encrypted communications over the telecommunications network" (claim 36). Accordingly, claims 7, 36, and 44 are also patentably distinguishable over Caputo et al. for the reasons set forth above.

The Office acknowledges that Caputo et al. does not disclose that the device sends the communications by wireless means, or that the device is enabled to use the enhanced wireless security of the Wireless Application Protocol, and relies on Grimm et al. and Geiger et al. as making up for these deficiencies. This reliance is unfounded because neither of the Grimm et

al. and Geiger et al. patents discloses an arrangement whereby a mobile communications device is capable of performing cryptographic functions for its own connection to a node via a wireless network, *and also* performing cryptographic functions for an external device (e.g., a computer) that is by itself capable of communicating over a computer network by means other than the mobile communications device, nor do either of the Grimm et al. and Geiger et al. patents disclose a computer relying on its own internal resources for some cryptographic functions and relying on the resources of a mobile communications device for other cryptographic functions. Therefore, any combination of Caputo et al. with Grimm et al. and Geiger et al. would still fail to include these various features.

For at least these reasons, claims 2, 3, 7, 10-18, 25, 29, 30, 35-40, 42, and 44 are believed to be patentable over the prior art of record. Accordingly, it is respectfully requested that the rejection of these claims under 35 U.S.C. §103(a) be withdrawn.

Claims 5, 8, 9, 23, 41, 46, and 49 stand rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over the combination of Caputo et al., Grimm et al., and Geiger et al. and further in view of Ericsson, "Bluetooth – A Global Specification for Wireless Connectivity." Also, claims 43, 45, and 50 stand rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over the combination of Caputo et al., Grimm et al., and Geiger et al. and further in view of RSA, "PKCS #11 v2.10: Cryptographic Token Interface Standard." These rejections are respectfully traversed.

Claim 23 has been canceled without prejudice or disclaimer, thereby rendering the rejection of this claim moot.

The remaining claims subject to these grounds of rejection variously depend from independent claims 1, 7, 36, 44, and 47 and are therefore patentably distinguishable over any combination of Caputo et al., Grimm et al. and Geiger et al. for at least the reasons set forth above.

In addition, the Office acknowledges that Caputo et al., Grimm et al., and Geiger et al. fail to disclose a wireless connection or connection via a short-range transceiver incorporating Bluetooth wireless technology, and relies on the Ericsson reference as making up for this deficiency. The Office further acknowledges that Caputo et al., Grimm et al., and Geiger et al. fail to disclose specifically that the mobile communications device utilizes PKCS #11 with AT commands, and relies on the RSA document as making up for this deficiency.

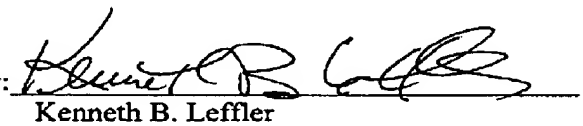
This reliance fails to support the rejections, however, because neither of the Ericsson or RSA documents discloses the various features discussed above with respect to the independent claims. Therefore, any combination of Caputo et al., Grimm et al., Geiger et al., Ericsson, and RSA would still fail to include all of the features defined by Applicant's claims.

For at least the foregoing reasons, claims 5, 8, 9, 41, 43, 45, 46, 49, and 50 are believed to be patentably distinguishable over the prior art of record. Accordingly, it is respectfully requested that the rejection of these claims under 35 U.S.C. §103(a) be withdrawn.

The application is believed to be in condition for allowance. Prompt notice of same is respectfully requested.

Respectfully submitted,
Potomac Patent Group PLLC

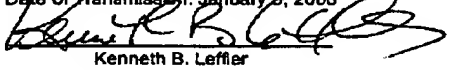
Date: January 5, 2006

By: 
Kenneth B. Leffler
Registration No. 36,075

P.O. Box 270
Fredericksburg, Virginia 22404
703-718-8884

I hereby certify that this correspondence is being sent by facsimile transmission to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 to the following facsimile number:

Facsimile Number: 571 273 8300
Date of Transmission: January 5, 2006


Kenneth B. Leffler